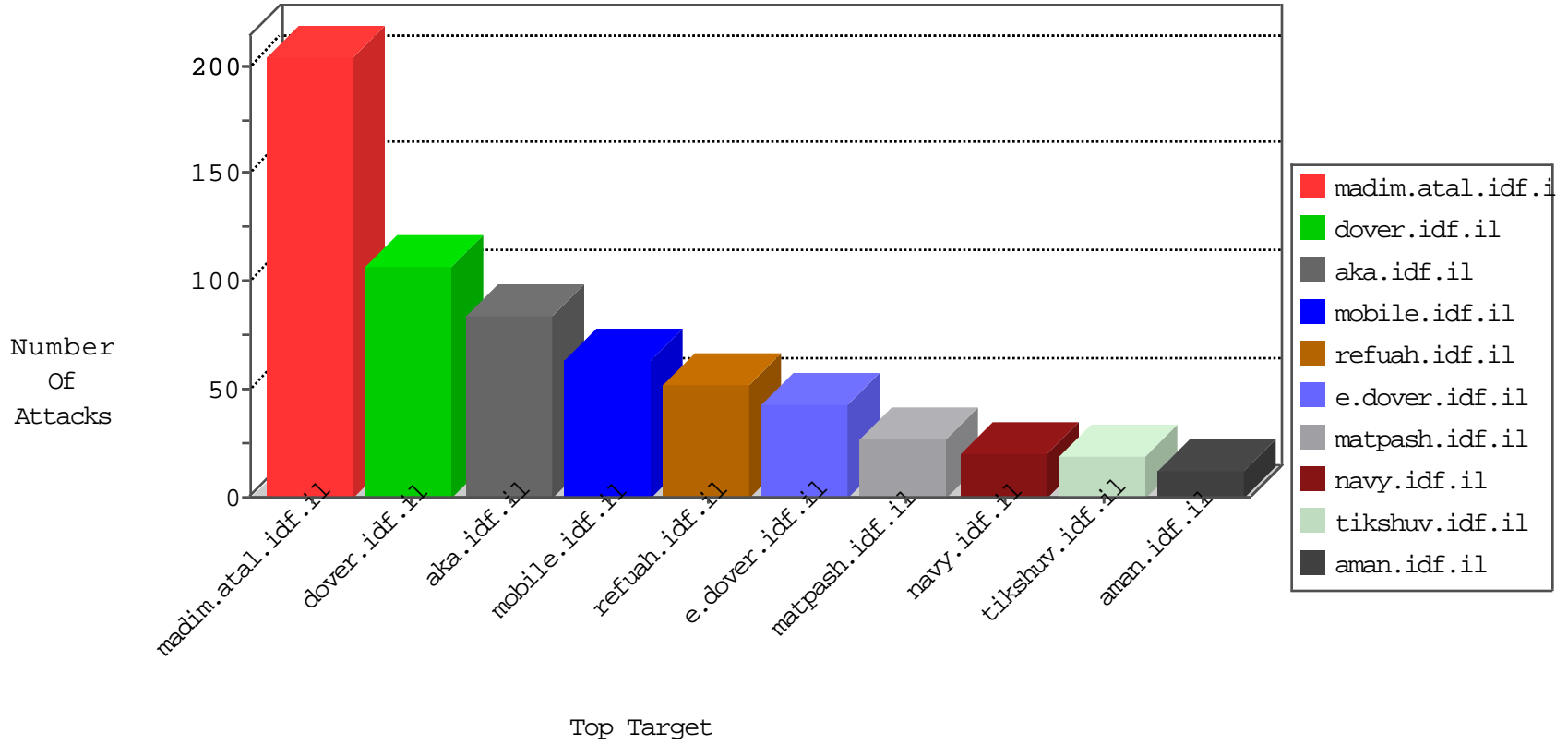


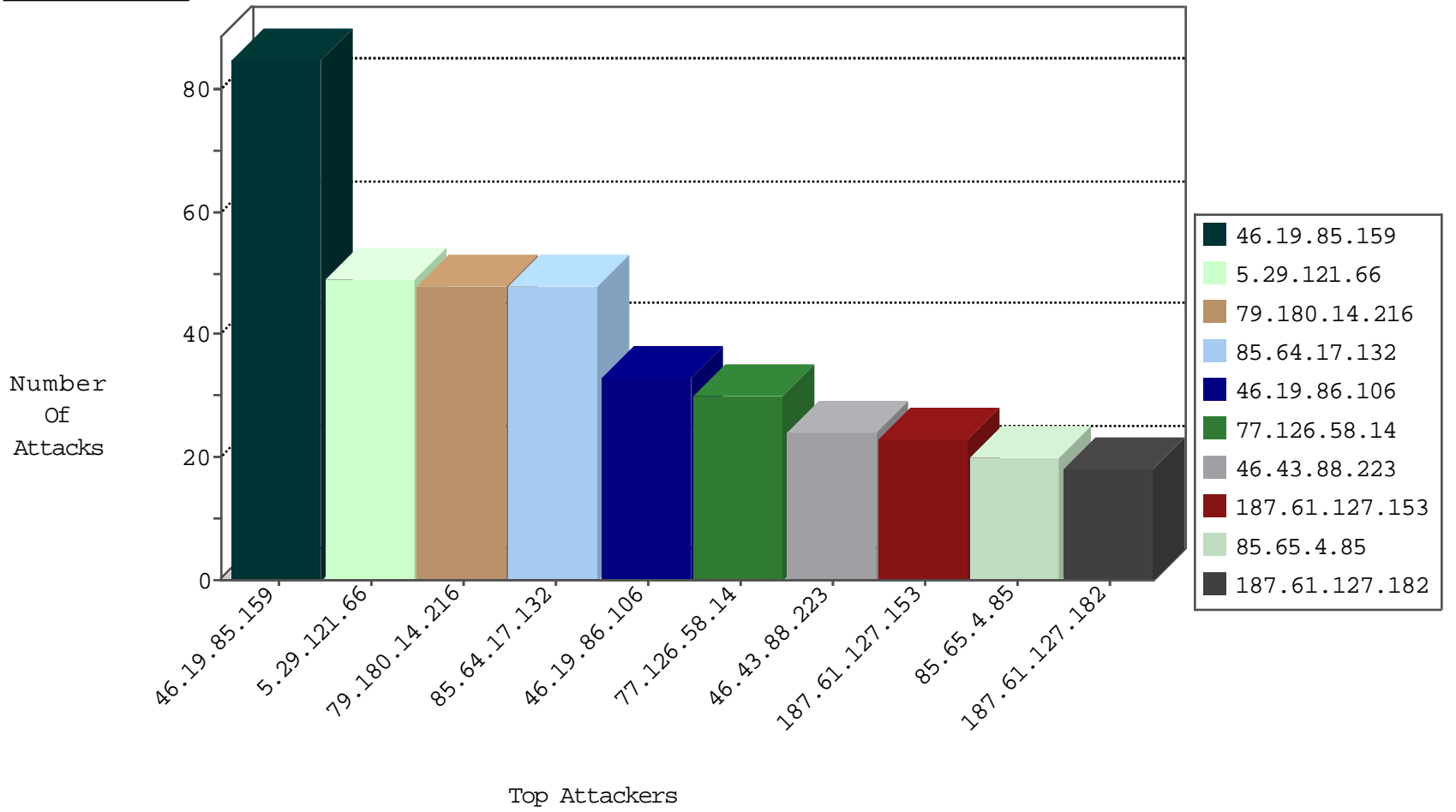
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
195.62.53.168	Russian Federation	147.237.76.30	himush.idf.il	block-sp-traf1	forward	2
209.126.136.2	United States	147.237.76.200	eitan.aka.idf.il	Black List	drop	1
139.0.18.6	Indonesia	147.237.76.202	e.halag.idf.il	I4 Source or Dest Port Zero	drop	1
185.94.111.1	Russian Federation	147.237.76.202	e.halag.idf.il	Black List	drop	1

10-04-2016-13:04:03 to 10-04-2016-14:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.76.31	nakchal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
163.172.238.45	147.237.77.178	United Kingdom	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
134.29.253.245	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
128.199.176.113	147.237.76.198	Singapore	e.yohalan.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
113.108.195.106	147.237.76.31	China	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
109.236.86.32	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
66.249.93.87	147.237.77.216	Europe	dover.idf.il	ET SCAN NMAP -sA (2)	1
62.210.243.100	147.237.77.233	France	atal.idf.il	ET SCAN NMAP -sS window 1024	1
14.125.246.49	147.237.76.177	China	ncore.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
201.194.100.214	147.237.76.34	Costa Rica	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
134.29.253.245	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
128.199.176.113	147.237.76.198	Singapore	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
119.140.150.236	147.237.77.234	China	halag.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
109.236.86.32	147.237.76.201	Netherlands	e.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
79.182.91.65	147.237.76.86	Israel	navy.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
66.249.93.85	147.237.77.216	Europe	dover.idf.il	ET SCAN NMAP -sA (2)	1
14.152.59.11	147.237.76.44	China	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
77.126.58.14	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
46.43.88.223	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	24
187.61.127.153	Brazil	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	23
85.65.4.85	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
187.61.127.182	Brazil	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	18
5.29.121.66	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
46.19.86.106	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
5.29.121.66	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	12
46.19.86.106	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
80.178.159.208	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
84.111.156.237	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
109.66.178.188	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
5.29.121.66	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
5.29.121.66	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
79.182.25.102	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
2.53.132.214	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
5.29.121.66	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
87.70.55.157	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.106	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.66.178.188	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	5
37.26.149.131	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	4
46.19.86.106	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
27.130.40.145	Thailand	147.237.77.74	law.idf.il	Header Rejection	header rejection pattern found in request	monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
94.156.237.50	Bulgaria	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
176.13.228.219	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.147.83	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
84.229.1.77	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
141.226.218.58	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
5.102.242.38	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
94.156.237.50	Bulgaria	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
2.55.10.149	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
213.8.204.67	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
5.102.254.11	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.253.212.225	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
46.19.86.241	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.253.202.188	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	2
46.210.190.101	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
46.19.85.115	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.120.122.219	Israel	147.237.77.74	law.idf.il	Command Injection	command injection detected in URL: 'label'	monitor	2
109.253.202.188	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
46.19.85.115	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
185.3.147.241	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.120.216.214	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
84.229.62.184	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
157.55.39.92	United States	147.237.76.200	eitan.aka.idf.	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
104.45.18.178	Netherlands	147.237.0.34	tikshuv.idf.il	Instant Messengers	instant messenger pattern found, application: Skype	monitor	2
46.19.86.224	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.85.115	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
37.26.149.131	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.159	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	85
85.64.17.132	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	48
79.180.14.216	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	48
2.53.155.70	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
85.64.157.242	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 85.64.157.242	Block	5
82.166.240.201	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
46.120.122.219	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/726-en/patzar.aspx200oktext/html34445<div class="default_image"></div> <div class="field field-name-field-title field-type-text field-label-hidden"><div class="field-items"><div class="field-item even">idf law review</div></div></div> 3200:00.359utf-8	Block	2
31.168.156.107	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl100\$ctl100\$cphMain\$TochenPlaceHolder\$btnSave in www.aka.idf.il/main/gyus/faq.aspx	None	1
87.70.55.157	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
77.139.102.150	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
66.249.76.61	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/.well-known/apple-app-site-association	Block	1
104.177.189.27	United States	147.237.72.166	aka.idf.il	NULL Character in Header Name at	Block	1
46.120.216.214	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
68.180.228.126	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation PageNum in www.tikshuv.idf.il/901-he/tikshuv.aspx	Block	1
66.249.64.109	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/apple-app-site-association	Block	1
141.226.218.58	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
46.4.74.42	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
104.131.92.125	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
66.249.76.62	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/.well-known/assetlinks.json	Block	1
104.177.189.27	United States	147.237.72.166	aka.idf.il	NULL Character in Method '[[#0]][[#0]][[#0]][[#19]]ñ	Block	1
46.121.148.63	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
85.64.50.90	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/gyus/authenticationervice.aspx/getauthuser	Block	1
68.180.228.238	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/apple-app-site-association	Block	1
176.15.244.249	Russian Federation	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on aka.idf.il/main/home/default.aspx	Block	1
46.19.85.25	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/nav.css	Block	1
104.177.189.27	United States	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Name	Block	1
80.178.159.208	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.76.80	Israel	147.237.0.16	my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on www.my-kosher-kravi.idf.il/robots.txt	Block	1
104.177.189.27	United States	147.237.72.166	aka.idf.il	Unknown HTTP Request Method '[[#0]][[#0]][[#0]][[#19]]ñ in URL	Block	1
52.16.137.212	Ireland	147.237.72.166	aka.idf.il	Unauthorized URL Access to /	Block	1
77.138.89.17	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https://www.aman.idf.il/	Block	1
66.249.69.67	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9712-he/refuah.aspx	Block	1
195.62.53.168	Russian Federation	147.237.76.30	himush.idf.il	Unauthorized URL Access to gmail.com/engine/log.txt	Block	1
104.177.189.27	United States	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Method '[[#0]][[#0]][[#0]][[#19]]ñ	Block	1
66.249.76.112	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/.well-known/apple-app-site-association	Block	1
109.66.178.188	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
66.249.64.78	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
5.102.242.38	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
85.64.157.242	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/gyus/kiosk/kiosk.aspx	Block	1
77.138.238.48	France	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1
66.249.75.60	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/1/1381.pdf	Block	1
212.106.82.97	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Parameter Type Violation fromDate in www.cogat.idf.il/901-ar/cogat.aspx	Block	1
104.177.189.27	United States	147.237.72.166	aka.idf.il	Malformed URL	Block	1
84.108.73.249	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/mobile/	Block	1
66.249.76.114	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/.well-known/assetlinks.json	Block	1
66.249.64.106	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/iturim/asp/displayallsoldiers.asp	Block	1
134.17.31.249	Belarus	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1